PENTEST PAINS

Chris Traynor

Ridgeback InfoSec, LLC

$ whoami

Chris Traynor

- Pentester at Black Hills InfoSec
- Owner of Ridgeback InfoSec, LLC
- Antisyphon Author/Instructor
  - Offensive Tooling Foundations
  - Offensive Tooling for Operators
  - BOTH now available via On-Demand**
- Certs: GSEC, GCIH, GWAPT, & GPEN

Why Is This Needed

- To get better. Plain and simple.

- Painful engagements have consequences
  - Less secure environments
  - Loss of revenue
  - Reputational harm (on both sides)
  - Litigation
  - Sometimes termination

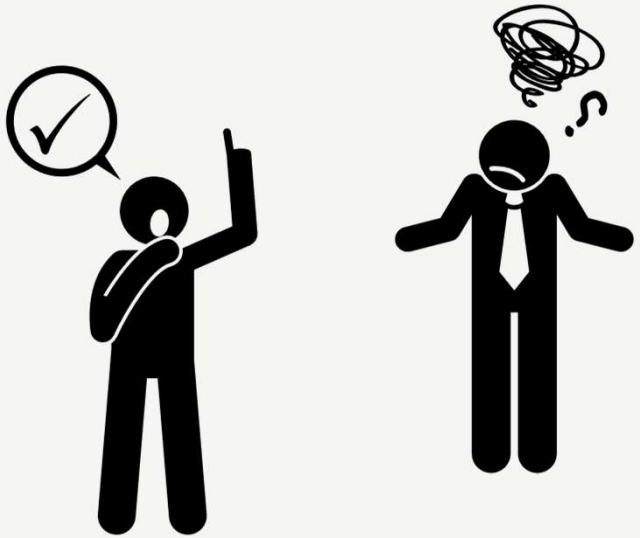
- This applies to ***everyone*** involved
  - Testers, POCs, SOC Analysts, Project Managers, etc.

- Keep in mind, MOST engagements go well

Define What You're Doing

- The hardest things to do in ***any*** job are **COMMUNICATION** & **EXPECTATION MANAGEMENT**
  - ...well...any office job at least

- Preconceptions & Misconceptions of Goals
  - Pentest
    - Web App, Network, Wireless, Physical, etc.
  - Red Team
  - Purple Team
  - Social Engineering
  - Phishing



Rules of Engagement (ROE)

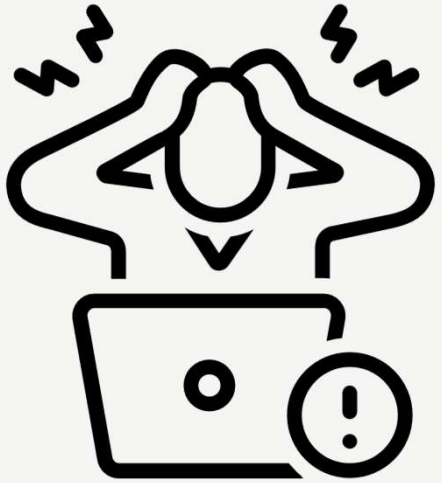
- Establish POCs on both sides AND identify backups
  - Vacations? PTO? Work related travel?
- Motivation for testing
- Confirm testing dates
- What's in-scope AND out-of-scope
- Define a communication cadence and medium
- Emergency scenario plan
- Get authorization for specific "high-risk" actions
- Assign action items
- Agree on due dates

Client-Driven Pain

- Inaccurate or confusing scoping
  - IPs, CIDR notation, FQDNs, etc.
  - Duplicated system listings
  - Often due to simply not knowing what they have
- Not adhering to RFC 1918
  - Class A: 10.0.0.0 to 10.255.255.255
  - Class B: 172.16.0.0 to 172.31.255.255
  - Class C: 192.168.0.0 to 192.168.255.255
- Not being ready on the agreed start date
  - “Environmental Preparedness for Testing” finding

Client-Driven Pain

- Being adversarial/taunting
- Threatening legal action early
- Insulting the tester personally or professionally
- Taking bad news badly
- Going dark during a test (unresponsive)
- Challenging ***every*** finding to get a “clean report”
- Having the wrong motivation
- Refusal to make concessions in the interest of more thorough testing
- Not giving timely feedback

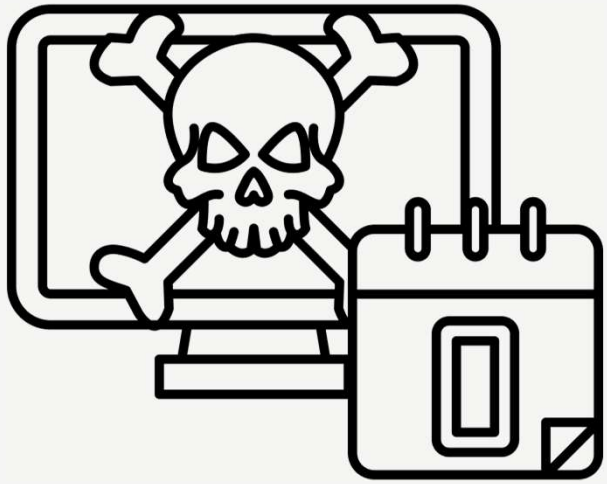


Tester-Driven Pain

- Not knowing your tools
  - Using the wrong tool for the job
  - Not realizing the full impact of a tool
- Not verifying the scope provided
- Not adhering to the out-of-scope list
- Attacking w/o regard for your customer's business type
  - Hospitals, ICS, etc.
- Running DoS exploits
- Being too proud to ask for help

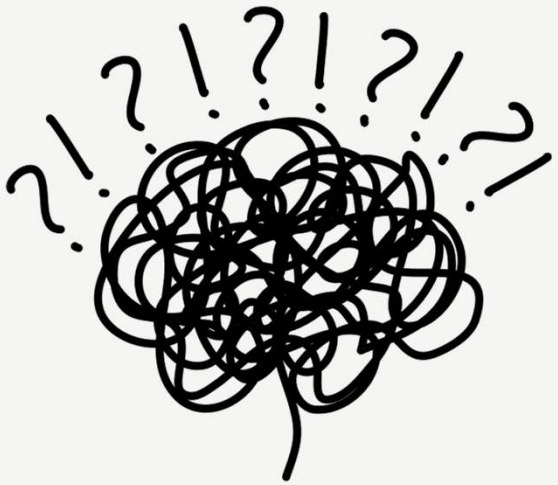
Tester-Driven Pain

- Not reporting as you go
  - **This is a big one folks!****
- Inaccurate reports and/or lack of evidence
- Not making the report actionable
- Taking on a test type you don't know well
  - It's alright to challenge yourself
  - But don't leave a client feeling let down
- Not communicating or not being responsive
- Missing deliverable due dates
- Being unethical or immoral
  - Know where to draw the line



When Things Go Wrong…

- Examples:
  - Indicators of Compromise
  - Critical findings
  - Errors in reports
- Remember, we're all on the same team
- Don't let ego get in the way
- Communicate quickly & professionally
- Document, document, and document
- Know when to escalate
- YOU don't *have* to be the bad guy



THANK YOU

FOR ATTENDING

Chris Traynor

blackhillsinfosec.com

antisyphontraining.com

ridgebackinfosec.com